UNIVERSIDADE DE BRASÍLIA
FACULDADE DE COMUNICAÇÃO
CURSO DE GRADUAÇÃO DE COMUNICAÇÃO ORGANIZACIONAL

HACKEANDO A PRIVACIDADE: UMA ANÁLISE DA POLÍTICA DE DADOS DO INSTAGRAM

Caroline Medeiros Miake

Brasília-DF
2022

Caroline Medeiros Miake

HACKEANDO A PRIVACIDADE: UMA ANÁLISE DA POLÍTICA DE DADOS DO INSTAGRAM

Trabalho de Conclusão de Curso apresentado na Faculdade de Comunicação da UnB como requisito parcial para a obtenção do grau de Bacharel em Comunicação Organizacional sob orientação do Professor Dr. Felipe Polydoro.

Brasília-DF
2022

Caroline Medeiros Miake

HACKEANDO A PRIVACIDADE: UMA ANÁLISE ACERCA DA POLÍTICA DE DADOS DO INSTAGRAM

Trabalho de Conclusão de Curso apresentado na Faculdade de Comunicação da UnB como requisito parcial para a obtenção do grau de Bacharel em Comunicação Organizacional sob orientação do Professor Dr. Felipe Polydoro.

Brasília, ____/____/_____

BANCA EXAMINADORA

_____

Professor Dr. Felipe Polydoro

Orientador

_____

Professora Dra. Mariah Sampaio

Membro 1

_____

Professora Dra. Janara Sousa

Membro 2

_____

Professora Dra. Elen Geraldes

Suplente

Dedico este trabalho à minha mãe, Francisca.

AGRADECIMENTOS

Passar pela experiência de me formar, trabalhar e viver no meio de uma pandemia, entre tantas crises de ansiedade, com certeza me fez uma pessoa mais forte. Posso dizer com o coração leve: até aqui o Senhor me sustentou. Agradecer não é sinônimo de que tudo correu bem, mas que mesmo dando errado, estarei com os olhos fixos naquilo que deu certo no final das contas. Por isso, meu primeiro “Muito obrigada” vai para o meu Pai porque foi Ele quem me colocou aqui e é Ele em quem tenho me apoiado em dias tão difíceis. Obrigada, Pai.

Não achava que seria possível admirar minha mãe mais do que já admiro, mas ela me surpreendeu nesta fase. Minha mãe é a mulher mais forte que tive a honra de conhecer. Também agradeço à Melissa por ser sempre tão amorosa, ao Dudu por ser tão animado, à Duda pela sua determinação, à minha avó que cuida mais de mim do que eu mesma, ao Marquinho por me apoiar nos meus estudos e ao meu pai por me proporcionar grandes ensinamentos.

Não posso me esquecer também de todos os amigos que fiz nessa caminhada universitária e ajudaram a tornar essa experiência ainda mais incrível. Agradeço à Patrícia Bezerra, à Fernanda Almeida, à Lara Silva, ao João Victor e ao Luiggi Fontenele. Obrigada por serem meus amigos. Em especial, agradeço à Júlia Nava por me ajudar tanto neste processo do TCC com livros, artigos e tantas outras dicas preciosas.

Agradeço também ao meu professor e orientador, Felipe Polydoro. Mal sabe ele o quanto o admiro! Obrigada pela paciência e os ensinamentos. Desejo ainda uma infinidade de boas experiências na tão honrada trajetória acadêmica.

Por fim, obrigada, Universidade de Brasília. Jamais me esquecerei dos meus momentos aqui.

“O choro pode durar uma noite, mas a alegria vem pela manhã.”

(Salmos, capítulo 30, versículo 5)

RESUMO

A vigilância digital está em constante evolução e a proteção da privacidade deve acompanhar este processo. Este artigo científico pretende compreender como a proteção de dados pessoais acontece neste cenário de monitoramento, especialmente na rede social Instagram. Os procedimentos metodológicos consistem na análise documental da Política de Dados do Instagram para compreender como a cultura de vigilância digital pode impactar a privacidade dos usuários do Instagram. Ao final, concluiu-se que as finalidades das coletas de dados nem sempre são claras e o usuário da rede social tem pouco domínio da circulação de suas informações.

Palavras-chave: Vigilância Digital. Privacidade. Dados Pessoais. Instagram.

ABSTRACT

Digital surveillance is constantly evolving and privacy protection must accompany this process. This scientific article intends to understand how the protection of personal data happens in this monitoring scenario, especially in the social network Instagram. The methodological procedures consisted of the documentary analysis of the Instagram Data Policy to understand how the culture of digital surveillance can impact the privacy of Instagram users. In the end, it was concluded that the purposes of data collection are not always clear and the social network user has little control over the circulation of their information.

Keywords: Digital surveillance. Privacy. Personal data. Instagram.

LISTA DE TABELAS

LISTA DE FIGURAS

SUMÁRIO

1 - INTRODUÇÃO

A realidade conectada tornou-se um território rotineiro rapidamente, antes mesmo que o usuário tomasse ciência de suas proporções e das diversas nuances que a era digital poderia alcançar. Desta forma, o ser humano presenciou uma mudança radical nas formas de se relacionar, trabalhar, estudar e comprar.

Dentro deste espaço digital um indivíduo deposita diariamente inúmeras informações sobre si mesmo. Informações estas que antes eram reservadas apenas na esfera pessoal, mas agora podem ser extraídas e mantidas eternamente em registros de computadores. Nesta perspectiva, *big data* é um termo muito utilizado para retratar essa massiva coleta de dados.

Muitas descrições tentam definir o *big data* de diferentes formas como uma tecnologia, um conhecimento ou um fenômeno. Dentre os muitos significados que a palavra pode conter, para Zuboff (2018, p.18), o *big data* seria um novo formato de capitalismo de vigilância com foco no uso das informações de forma intencional e com grandes consequências, com capacidade de prever o comportamento humano através dos dados coletados e influenciá-lo para benefício do mercado.

> O big data é constituído pela captura de small data, das ações e discursos, mediados por computador, de indivíduos no desenrolar da vida prática. Nada é trivial ou efêmero em excesso para essa colheita [...] Esses dados são adquiridos, tornados abstratos, agregados, analisados, embalados, vendidos, analisados mais e mais e vendidos novamente (ZUBOFF, 2018, p. 31).

Diante da perspectiva da cultura de vigilância digital e do monitoramento de mídia, existe o estímulo da produção social, a geração constante de conteúdo para as redes sociais e o desejo persistente em estar sempre online. Desta forma, o usuário da internet deixa seus rastros digitais a cada pesquisa feita no Google, mensagens instantâneas deixadas em aplicativos, em postagens que viralizam em tempos recordes ou comentários realizados em qualquer site.

A privacidade assume novas faces e levanta novas questões sobre ceder informações pessoais e permitir-se ser vigiado pelas novas tecnologias de monitoramento digital. Neste contexto, a privacidade não diz respeito a esconder-se, mas ter o domínio de qual e de como a informação é transmitida.

Atualmente no Brasil, existe a Lei de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709/2018. A LGPD legisla acerca do tratamento de dados pessoais em todos os meios, inclusive o digital. Ou seja, existe uma série de determinações jurídicas e

normas acerca das informações coletadas por parte das organizações, especialmente no meio digital.

Neste contexto, as mídias sociais têm crescido exponencialmente nos últimos anos. De acordo com a pesquisa da We Are Social e Hootsuite de janeiro de 2022[1], existem 4,95 bilhões de usuários da internet ao redor do mundo e 4,62 bilhões estão nas redes sociais ativamente. Dentre as muitas redes sociais utilizadas, o Instagram ocupa a posição de 4º lugar, atrás apenas do Facebook, Youtube e Whatsapp, respectivamente. Todas as 4 redes sociais pertencem ao Meta, antes denominada Facebook.

Dentro desta perspectiva, este artigo pretende responder: Como a cultura de vigilância digital pode impactar a privacidade dos usuários do Instagram? O principal objetivo é entender quais são os dados coletados e como são tratados através da Política de Dados do Instagram. Para chegar a este fim, o artigo será estruturado em cinco partes: A Cultura da Vigilância Digital; Proteção de Dados Pessoais na Internet; Repensando a Privacidade; Procedimentos Metodológicos; Análise da Política de Dados do Instagram; e Conclusão.

No primeiro capítulo os principais conceitos de *big data*, monitoramento de mídia e vigilância digital serão estudados. O segundo capítulo trará aspectos da proteção de dados pessoais no contexto da democracia no Brasil. Já o terceiro capítulo dispõe de reflexões acerca das nuances da privacidade no âmbito da realidade do monitoramento digital e exposição na internet.

Para os Procedimentos Metodológicos, quinto capítulo deste artigo, serão apresentados os meios para a realização da análise documental da Política de Dados do Instagram. No sexto capítulo serão estudados três eixos principais que consistem em: Monitoramento Digital, Coleta e Capitalização e Autodeterminação Informativa. Dentro desta perspectiva, parâmetros como clareza da informação, características da privacidade, formato de tratamento de dados e aspectos da vigilância digital serão observados. Além disso, essa análise também contará com a pesquisa bibliográfica realizada ao longo dos demais capítulos para o embasamento teórico. Por fim, na Conclusão serão feitas as discussões acerca da análise realizada.

[1] "*The Global State of Digital 2022*". Disponível em <https://www.hootsuite.com/pt/recursos/digital-trends>. Acesso em: 29 mar. 2022.

2 - A CULTURA DA VIGILÂNCIA DIGITAL

Uma distopia futurística escrita por George Orwell em 1949 tornou-se um fenômeno na época ao retratar o famoso *Big Brother*[2], uma metáfora de um poder cruel, invasor da privacidade de seu povo. O livro denominado 1984, apesar de ser um clássico da ficção, apresenta algumas semelhanças com a realidade do século XXI. Para Solove (2006, p. 29), a problemática dos bancos de dados é frequentemente descrita de acordo com o conceito do Big Brother orwelliano, "Um governo onisciente e constantemente vigilante que regula todos os aspectos da existência de alguém"[3].

Apesar de o panorama atual de vigilância não retratar este formato totalitário e centralizado, a metáfora orwelliana traz discussões valiosas acerca da privacidade e vigilância. O que a distopia de 1984 não antecipou foram os "*Little Brothers*"[4] (SOLOVE, 2006, p. 32) do sistema descentralizado corporativo com foco na monetização. "A visão distópica de Orwell era dominada pelo estado central. Ele nunca adivinhou o quão significativo um consumismo descentralizado pode se tornar para o controle social" (LYON, 1994, p. 78 *apud.* SOLOVE, 2006, p. 32).

A prática da vigilância remonta a um período muito antes da tecnologia hodierna. Fernanda Bruno (2008, p. 11) lembra que o termo "censor" deriva-se da história social dos números da civilização romana. Os homens eram contabilizados para fins de taxação, obrigações militares, status políticos, censura e controle dos hábitos.

> Somos herdeiros dessa maquinaria, ainda presente entre nós, mas ela é atravessada por novos processos e tecnologias que não apenas apontam a intensificação de mecanismos passados, como a emergência de modelos diferenciados de monitoramento e coleta dos dados (BRUNO, 2008, p. 11-12).

A vigilância digital se caracteriza por "um monitoramento sistemático, automatizado e à distância de ações e informações de indivíduos no ciberespaço" (BRUNO, 2008, p. 11). Por mais que a vigilância e o monitoramento existam há muito tempo e de formas variadas, os limites ainda estão em processo de serem definidos entre aquele que cede a informação e aquele que a detém. Para a autora (2008, p.11), é possível destacar quatro processos comuns da vigilância digital: os mecanismos de

[2] Grande Irmão. Tradução nossa.
[3] No original: "*an all-knowing, constantly vigilant government that regulates every aspect of one's existence*". Tradução nossa.
[4] Pequenos Irmãos. Tradução nossa.

coleta, monitoramento e arquivo de informação; os sistemas de classificação e conhecimento dos dados; os procedimentos de individualização e produção de identidades; as formas de controle sobre as ações e escolhas dos indivíduos.

Shoshana Zuboff (2018, p. 22) trata a realidade deste cenário como a nova lógica de acumulação digital. Para a autora, o poder desta acumulação é tácito, com a capacidade de moldar o campo das possibilidades conforme for desejado: define objetivos, sucessos, fracassos, problemas, o que deve ser valorizado e desprezado, organizado ou espalhado.

Quanto mais bem definidos e explorados forem estes processos, maior a vantagem competitiva no mundo corporativo. Estima-se que 90% dos dados do mundo tenham sido criados apenas nos últimos dois anos (Oracle, 2022)[5]. Desta forma, o *big data* - ou "grandes dados" - configura-se como um sistema muito mais complexo de análise massiva de dados coletados na web.

Para o Grupo Gartner (2022)[6], o *big data* é tido como "ativos de informação de alto volume, velocidade e variedade, considerada uma nova forma econômica e inovadora de processamento de informações". A prática de extração, análise e manipulação corroboram para uma realidade de constante vigilância digital e monitoramento de mídia no século XXI, visto que qualquer informação coletada pode se tornar valiosa para o mercado.

Lyon (2018) refere a esta realidade como cultura da vigilância, algo que os cidadãos aceitam deliberadamente e frequentemente sem questionar:

> O que antes era um aspecto institucional da modernidade ou um modo tecnologicamente aperfeiçoado de disciplina ou controle social hoje está internalizado e constitui parte de reflexões diárias sobre como são as coisas e do repertório de práticas cotidianas (LYON, 2018, p. 153).

Informações coletadas no ciberespaço podem revelar onde determinada pessoa estava e com quem, identificar problemas de saúde e condições financeiras através de uma simples pesquisa no Google. A evolução da tecnologia dos dispositivos *smart*, assim como a amplificação da presença humana online, colaboram para um sistema unificado e benéfico para o monitoramento digital.

[5] "O que é Ciência de Dados?" Disponível em <https://www.oracle.com/br/data-science/what-is-data-science/> Acesso em: 09 mar. 2022.
[6] "Gartner Glossary". Disponível em <https://www.gartner.com/en/information-technology/glossary/big-data> Acesso em: 09 mar. 2022.

Fernanda Bruno (2008, p. 12) define dois modelos de dados: os estáveis e os circunstanciais. O dado estável consiste nas informações com pouca ou nenhuma alteração no decorrer do tempo, como nome, dados geodemográficos, biométricos, entre outros. Já o dado circunstancial muda constantemente, são os dados comportamentais, transacionais, psicológicos, sociais, entre outros. Para a autora, essa segunda categoria é onde a vigilância digital é mais expressiva.

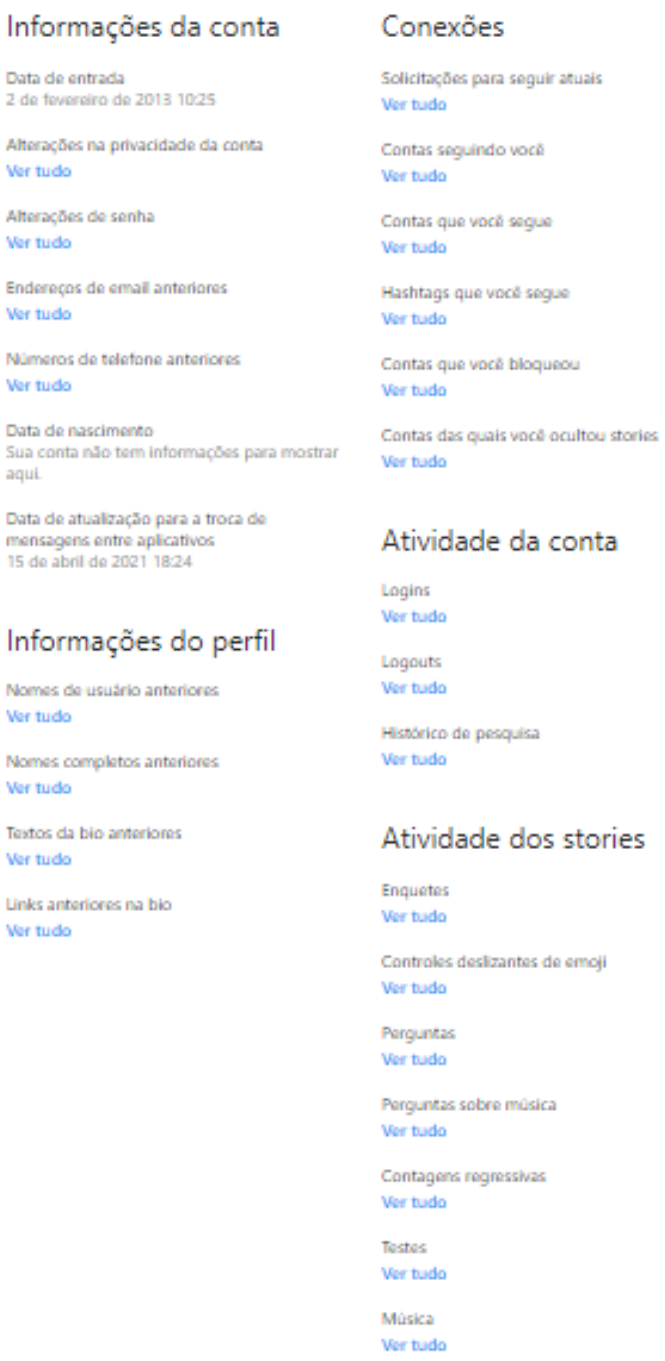
Quanto mais informações extraídas, melhor será a análise e utilização desses dados por parte das corporações. Em entrevista para a BBC, o doutor em Comunicação, Economia e Ciências Sociais, Martin Hilbert, afirmou "com 250 likes; o algoritmo do Facebook pode prever sua personalidade melhor que seu parceiro"[7]. Lyon (2018) também enfatiza a perspectiva de que o usuário também é responsável pelo próprio processo de vigilância:

> Somos cúmplices, como jamais antes, em nossa própria vigilância ao compartilhar – por vontade própria e conscientemente ou não – nossas informações pessoais no domínio público online (LYON, 2018, p. 154).

A título de exemplo, nas configurações de "Privacidade e Segurança" do Instagram é possível encontrar parte de alguns dados extraídos pela rede social individualmente, conforme imagem abaixo.

[7] 'Despreparada para a era digital, a democracia está sendo destruída', afirma guru do 'big data'. Disponível em <https://www.bbc.com/portuguese/geral-39535650>. Acesso em 10 mar 2022.

Figura 1 - Configurações de Privacidade e Segurança do Instagram



Fonte: Instagram[8].

É neste contexto em que os profissionais especializados, *data brokers*[9] ou "agentes de informação", ganham espaço. Esta área coleta e rastreia informações de

[8] Print realizado na conta pessoal do Instagram da autora.
[9] "Data Brokers: Tudo o que você precisa saber". Disponível em <https://www.avast.com/pt-br/c-data-brokers>. Acesso em: 11 mar. 2022.

todos os tipos através de Cookies, scripts, web beacons, endereços de IP, sites de comércio eletrônico, entre outros. Existem medidas legislativas ao redor do mundo que tentam regulamentar esta prática, mas ainda é pouco desenvolvida na maioria dos casos.

O relatório *Data Brokers: A Call for Transparency and Accountability* elaborado pela Federal Trade Comission de 2014, realizou um mapeamento acerca da indústria de dados e como os *data brokers* operam. Mesmo sendo relativamente antigo, o documento traz reflexões importantes para a realidade do monitoramento digital. Ana Frazão (2019) resumiu as conclusões do relatório da seguinte forma:

> (i) os data brokers coletam informações sobre os consumidores de diversas e numerosas fontes comerciais, governamentais e públicas (incluindo nesta últimas mídias sociais, blogs e internet);
> (ii) os data brokers não usam apenas os dados crus (raw data), mas também os chamados dados derivados, que são as inferências já realizadas a partir dos dados crus;
> (iii) os data brokers combinam dados obtidos on-line e off-line para atingirem os consumidores on-line;
> (iv) as principais utilizações comerciais dos dados são marketing, serviços de mitigação de riscos e serviços de busca de pessoas;
> (v) parte expressiva da coleta de dados ocorre sem o conhecimento dos consumidores;
> (vi) a indústria dos dados é complexa, com muitas camadas de data brokers que oferecem e trocam dados uns com os outros, sendo frequentes o intercâmbio e a compra e venda de informações entre eles;
> (vii) os data brokers coletam e armazenam bilhões de dados que, na época da pesquisa, já cobriam praticamente todos os consumidores norte-americanos;
> (viii) qualquer que seja a metodologia utilizada, os data brokers coletam mais informações do que usam;
> (ix) uma das maiores aplicações dos dados é o desenvolvimento de modelos complexos para predizer o comportamento dos consumidores e para extrair inferências potencialmente sensíveis a respeito deles;
> (x) apesar dos benefícios da atividade de tratamento de dados, muitos dos propósitos pelos quais os data brokers coletam e usam dados apresentam riscos para os consumidores;
> (xi) as escolhas que os data brokers oferecem aos consumidores sobre os seus dados são invisíveis e incompletas, com grande ausência de transparência (FRAZÃO, 2019, p. 29-30).

Posto isto, o cenário de vigilância e monitoramento está em constante mutação e evolução. Por estar intrinsecamente relacionado com o sujeito, este torna-se participante cada vez mais ativo desta cultura e não apenas alvos ou portadores de vigilância (LYON, 2018, p. 159). Desta maneira, a proteção dos dados pessoais é imprescindível e, além de tudo, um direito.

3 - PROTEÇÃO DE DADOS PESSOAIS NA INTERNET

A cultura da vigilância tem corroborado para este novo mercado lucrativo, principalmente para grandes corporações. Em 2017, a revista The Economist, publicou uma manchete em sua capa com o título “A fonte mais valiosa do mundo” e “Dados e as novas regras da competição”[10] como subtítulo, com destaque para grandes empresas como Amazon, Uber, Microsoft, Google, Facebook e Tesla na imagem.

Figura 2 - Capa The Economist de 06 de maio de 2017

Fonte: The Economist, 2017.

Pode-se observar este fato, por exemplo, com o caso da Cambridge Analytica. Em 2018, Mark Zuckerberg, fundador da empresa Meta, precisou depor diante de um comitê legislativo depois de ser acusado de expor informações de bilhões de usuários do Facebook – sem o consentimento – para a empresa de análise de dados Cambridge Analytica, que trabalhou com Donald Trump nas eleições norte-

[10] *“The World’s most valuable resource* e *Data and the new rules of competition”*. Tradução nossa. Disponível em <https://www.economist.com/weeklyedition/2017-05-06>. Acesso em: 10 mar. 2022.

americanas de 2016[11]. Os dados coletados foram extraídos através da rede social e posteriormente vendidos para serem usados na campanha de Trump.

> Ao clicar em fazer o teste pelo Facebook, contudo, quase a totalidade dos usuários (aqueles que não leram os termos e condições da pesquisa e a política de privacidade do aplicativo) dava acesso à CA [Cambridge Analytica] para coletar os seus dados pessoais – a título exemplificativo: idade, cor, religião, altura, região onde o indivíduo reside e trabalha, sua geolocalização, por onde você costuma caminhar, seu passo de caminhada, acesso a todas as suas postagens, fotos e arquivos que foram colocados nessa rede social (FORNASIER E BECK, 2020, p. 188).

Tais informações foram usadas com o objetivo de catalogar o perfil das pessoas. Desta forma, seria possível direcionar conteúdo personalizado e materiais pró-Trump para os perfis específicos. Apesar de precisar pagar uma multa de 5 bilhões de dólares[12] dada pela Comissão Federal de Comércio dos Estados Unidos, não chega a ser comparável à capitalização de mercado do Facebook - agora Meta - de 575 bilhões de dólares na época.

Em uma outra ocasião, no início de 2022, Mark Zuckerberg ameaçou retirar os aplicativos Instagram e Facebook da Europa após as autoridades reguladoras recusarem cláusulas de transferência de dados europeus para os Estados Unidos[13]. Situações semelhantes a essas têm acontecido cada vez mais na era da hiperconectividade, especialmente entre grandes empresas como as representadas pelo *The Economist* em sua capa: Meta, Google, Amazon, entre outras. Posto isto, o direito de privacidade tem se revelado primordial para a democracia na sociedade digital.

Para Ana Frazão (2019, p. 24), o fenômeno da economia movida a dados não se restringe apenas à esfera do capital, mas tornou-se transversal, inclusive ao repercutir nas relações sociais e políticas também. A realidade da sociedade digital de extração de dados tem o potencial de colocar em risco valores fundamentais da individualidade e privacidade. Os autores, Olivieri e Castro (2021, p. 34), afirmam que o cidadão precisa que esta nova ordem social funcione sob a lei e sobre a autoridade

[11] "Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades". Disponível em <https://www.bbc.com/portuguese/internacional-43461751> Acesso em: 09 mar. 2022.

[12] "EUA multam Facebook em 5 bilhões de dólares por violar privacidade dos usuários". Disponível em <https://brasil.elpais.com/brasil/2019/07/12/economia/1562962870_283549.html>. Acesso em: 09 mar. 2022.

[13] "Por dados, Meta ameaça tirar Facebook e Instagram da Europa". Disponível em: <https://exame.com/negocios/por-dados-meta-ameaca-tirar-facebook-e-instagram-da-europa/>. Acesso em: 09 mar. 2022.

de uma governança democrática. Caso contrário, a exploração econômica de tratamento de dados pessoais deixaria o ser humano à mercê do mundo corporativo.

> Efeitos nefastos para a vida democrática e o sistema democrático de governo, pois nos tornaríamos uma espécie de colméia ou rebanho dirigido pelas empresas de tecnologia digital e pastoreado pelos sacerdotes dos saberes da informática (OLIVIERI E CASTRO, 2021, p. 36).

Nesta perspectiva, a realidade de extração de dados é unidirecional e não um relacionamento (ZUBOFF, 2018, p. 33). Consequentemente, aquele que toma a informação obtém muitos saberes a respeito daquela pessoa e o titular dos dados, praticamente nada do responsável pela coleta. A violação da privacidade e dos dados torna-se um ciclo interminável baseado na extração e monetização das informações coletadas.

Figura 3 - Ciclo do Mercado de Dados

Fonte: FRAZÃO, 2019, p. 29.

Existem frases padrão utilizadas pelas políticas de dados ou de privacidade afirmando que a troca de informações é essencial para uma experiência melhor e mais vantajosa para o usuário. Desta forma, a troca torna-se um princípio basilar para a utilização dos serviços online.

> Até a forma como a questão é apresentada já reflete a perspectiva utilitarista que permeia a análise, pois se parte da premissa de que, em nome da inovação, é justificável o sacrifício de direitos fundamentais elementares (FRAZÃO, 2019, p. 31).

A premissa da inovação faz com que a exploração dos dados seja justificada diante do comprometimento da individualidade e privacidade online. A extração torna-se ainda mais invasiva ao monitorar personalidade, propensão do indivíduo, estado emocional, antever doenças e distúrbios e outros similares. Abaixo um exemplo de como a Política do Instagram apresenta essa questão:

> **Pesquisa e inovação.**
> Usamos as informações que temos para estudar nosso Serviço e colaborar com terceiros em pesquisas para tornar nosso Serviço melhor e contribuir para o bem-estar de nossa comunidade (Instagram, 2022).[14]

Inegavelmente a tecnologia e seus avanços têm contribuído de diversas formas para a sociedade na ciência, no entretenimento, na educação. A questão torna-se problemática a partir do momento em que a privacidade torna-se “moeda de troca” e o indivíduo passa a não ter controle sobre informações que dizem respeito a ele mesmo e em como estas são utilizadas.

> [...] uma vez que os algoritmos – ou aqueles que os criam e os utilizam – tanto podem determinar os destinos das pessoas como também podem ser desenhados para influenciar e modificar o comportamento humano. O conhecimento profundo das características do usuário, inclusive no que diz respeito às suas fragilidades, pode ser utilizado para toda sorte de discriminações e abusos, além da manipulação de suas emoções, crenças e opiniões para os fins mais diversos, inclusive políticos (FRAZÃO, 2019, p. 37).

Posto isto, a legislação brasileira tem tomado providências acerca da privacidade na internet e suas problemáticas correspondentes com a Lei Geral de Proteção de Dados Pessoais (LGPD). A Lei nº 13.709 foi sancionada em 2018 e entrou em vigência em 2020 no Brasil. A partir da LGPD, o tratamento de dados pessoais passou a ser regulamentado, tendo como um dos seus objetivos, proteger os direitos fundamentais de liberdade e de privacidade.

O Art. 2º da Lei 13.709, de 14 de agosto de 2018, apresenta os fundamentos da proteção de dados pessoais. São eles: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; os direitos humanos, o livre desenvolvimento

[14] Termos de Uso do Instagram. Disponível em <https://web.facebook.com/help/instagram/581066165581870/?helpref=hc_fnav> Acesso em: 14 mar. 2022.

da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (Brasil, 2018).

A Lei não se resume apenas ao ambiente digital, mas parte expressiva do tratamento de dados atualmente é realizada por meios online. Apesar da legislação brasileira penalizar o tratamento irresponsável de acordo com suas diretrizes, as empresas frequentemente buscam alternativas para contornar tais impedimentos. A título exemplificativo, o caso da *Cambridge Analytica* citado no capítulo anterior.

O artigo 9º da LGPD também prevê uma série de critérios sobre como deve ser realizado o tratamento de dados por parte do controlador e determina quais são as informações que o titular deve ter acesso de forma clara, adequada e ostensiva:

> I - finalidade específica do tratamento;
>
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
>
> III - identificação do controlador;
>
> IV - informações de contato do controlador;
>
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
>
> VI - responsabilidades dos agentes que realizarão o tratamento; e
>
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei (Brasil, 2018).

Tais critérios são relevantes para garantir a adequação das empresas ante a realidade de tratamento de dados. Nesta perspectiva, é também necessário compreender o novo panorama em que a privacidade está inserida na era digital.

4 - REPENSANDO A PRIVACIDADE

O acesso aos dados pessoais é um “mal necessário” quando se fala da utilização de redes sociais. Ceder diversas informações em troca da experiência, da utilidade e do entretenimento proporcionado pelo serviço disponibilizado pela empresa faz parte do seu contrato de uso. Desta forma, aceitar os Termos de Uso - que estão sempre linkados com suas respectivas políticas - é uma das primeiras ações a serem executadas quando um novo usuário realiza o cadastro.

Compreender como as políticas funcionam e se os Termos de Uso são apropriados ou não é primordial, afinal dificilmente um indivíduo assina um contrato

sem antes lê-lo. Todavia, não é o que acontece em uma realidade digital e informações importantes acabam sendo distribuídas livre e deliberadamente, muitas vezes sem a responsabilidade que lhe é devida.

Para a autora, Carissa Véliz (2021), privacidade é poder. É comum um indivíduo afirmar não se importar com a vigilância digital, por não ser uma pessoa relevante, por não ser uma figura pública ou uma celebridade. Entretanto, cada dado extraído pode, de fato, se tornar imensamente relevante quando se torna um potencial voto nas urnas ou para um investimento em determinado negócio. Assim, uma pessoa pode ter grande poder em mãos ao disponibilizar seus dados pessoais que podem ser fundamentais para situações como estas.

> Imagine ter uma chave mestra para a sua vida: uma chave ou senha que lhe dá acesso à porta da frente de sua casa, seu quarto, sua agenda, seu computador, seu telefone, seu carro, seu cofre e seus registros de saúde. Você andaria por aí fazendo cópias dessa chave e entregando-as a estranhos? Provavelmente, não. Então, por que você está disposto a entregar seus dados pessoais a praticamente qualquer pessoa que os solicite? (VÉLIZ, 2021, p. 94).

Ao tomar como base a realidade dos *data brokers*, citados no capítulo 1[15] neste artigo, é possível visualizar como opera este monitoramento nas redes sociais e quais seus objetivos. Uma das características não só da vigilância digital, mas também da realidade globalizada do século XXI, é a capacidade do mercado em capturar e transformar qualquer oportunidade em mercadoria, inclusive a privacidade (SIBILIA, 2016, p. 14).

Compreender os conceitos de transparência e como esta se contrasta com a privacidade é primordial para assimilar o modo como os *Little Brothers* utilizam esta realidade a seu favor. Para Solove (2006, p. 143), a transparência e a privacidade caminham juntas numa complexa relação paradoxal: ou a informação disponível é completamente pública ou completamente sigilosa.

A privacidade exige que exista um certo nível de limite na disponibilização dessas informações, mas a transparência pede clareza sob todos os ângulos daquilo que está em tópico de análise. Todavia, Solove revela a importância de se encontrar o equilíbrio entre os dois conceitos.

> Se abandonarmos a noção de que a privacidade é um status exclusivo e reconhecermos que informações em registros públicos ainda podem permanecer privadas, mesmo que haja acesso limitado a ele, então podemos encontrar um compromisso viável para a tensão entre transparência e

[15] Capítulo 1, p. 20.

> privacidade. Podemos fazer a informação acessível apenas para determinados fins[16] (SOLOVE, 2006, p. 150).

A transparência das informações tem a capacidade de promover benefícios à sociedade como, por exemplo, no controle de crimes. Entretanto, informações pessoais podem ser utilizadas para finalidades não antes acordadas ou informadas e é onde a violação do direito de privacidade se concretiza.

Stefano Rodotà (2008, p.25) observa que o conceito de privacidade deve ser amplificado e não mais levar em consideração a visão dicotômica entre a “casa-fortaleza” - que glorifica a privacidade e favorece o egocentrismo - e “casa-vitrine” - que privilegia as trocas sociais - no contexto da sociedade digital. De acordo com o autor, estas tendem a ser alternativas cada vez mais abstratas.

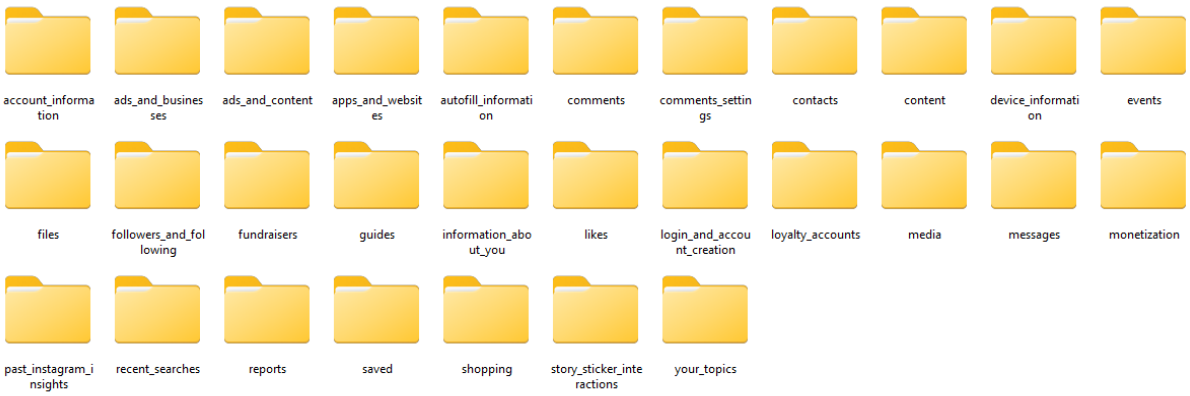
Grande parte da disponibilização em massa de dados na internet se dá por conta da própria inclinação do usuário em expor suas realidades na web. A hiperconectividade tornou-se solo fértil para a produção de conteúdo e amplificação dos relacionamentos nas mais variadas esferas da sociedade.

> A visibilidade e a conexão sem pausa constituem dois vetores fundamentais para os modos de ser e estar no mundo mais sintonizados com os ritmos, os prazeres e as exigências da atualidade, pautando as formas de nos relacionarmos conosco, com os outros e com o mundo (SIBILIA, 2016, p. 20).

Para exemplificar essa disposição de informações, em uma das funcionalidades disponibilizadas pelo Instagram[17], o usuário é capaz de realizar o download de informações extraídas pela rede social. Neste relatório, é possível identificar as seguintes pastas com os seguintes dados do usuário:

[16] Tradução nossa.
[17] Esta funcionalidade está disponível apenas no Instagram Web.

Figura 4 - Download de informações extraídas pelo Instagram



Fonte: Instagram.[18]

O conteúdo das pastas envolve: informações da conta; ads e business; ads e conteúdo; apps e websites; informações automáticas; comentários; configurações de comentários; contatos; conteúdo; informações de dispositivo; eventos; arquivos; seguidores e seguidos; arrecadação de fundos; guias; informações sobre você; curtidas; login e criação de conta; contas leais; mídia; mensagens; monetização; insights passados do instagram; pesquisas recentes; relatório; salvos; compras; adesivos de storys e interações; seus tópicos[19].

A transparência, em alguns casos, acaba levando a privacidade no limite ou além dele. No caso do Instagram percebe-se como o monitoramento digital extrai tanto os dados estáveis como os circunstanciais. Por exemplo, no caso da pasta “seus tópicos” onde são coletadas informações sobre conteúdos relacionados com as emoções do usuário. É possível observar também as coletas acerca de publicidades e propagandas, um dos principais agentes da capitalização dos dados.

Diante do exposto, percebe-se a importância de uma regulamentação no que tange a privacidade de dados. Assim, informações pessoais extraídas pelo Instagram ou qualquer outra rede social, sejam utilizadas para outros fins ou por terceiros, além de garantir ao indivíduo a autodeterminação informativa (COSTA, OLIVEIRA, 2019, p. 28-29). Ou seja, que a própria pessoa tenha domínio e ciência de como suas informações estão sendo tratadas, e ainda, a possibilidade de encerrar este tratamento caso não o ache apropriado.

[18] Print realizado pela autora.
[19] Tradução das pastas realizada pela autora.

5 - PROCEDIMENTOS METODOLÓGICOS

Este artigo se propôs a analisar a Política de Dados do Instagram a fim de observar a configuração e adequação da rede social diante da realidade da cultura de vigilância digital ao levar em consideração a proteção de privacidade do usuário no ciberespaço. O Instagram foi escolhido por ser uma das redes sociais pertencentes ao Meta, uma das maiores empresas de tecnologia atualmente e que já se envolveu em escândalos relacionados a vazamento ou vulnerabilidade de dados. Paralelo a isto, de acordo com a pesquisa da We Are Social e Hootsuite de 2022[20], o Instagram ocupa a posição de 4º lugar entre as plataformas mais usadas do mundo, atrás apenas do Youtube, WhatsApp, e Facebook, respectivamente. Todas as 4 redes sociais pertencem ao Meta, entretanto o Instagram está em 2º lugar entre as redes sociais favoritas dos usuários. Ou seja, esta rede social com uma grande quantidade de usuários e de grande relevância para o cenário virtual necessita de uma Política de Dados adequada para seu porte.

A Política de Dados do Instagram está disponível na web[21] e no aplicativo de celular para ser acessada a qualquer momento. Para Gil (2008, p.147), as fontes documentais proporcionam dados em quantidade e qualidade, capazes de contribuir para a investigação de determinado fato ou fenômeno. Desta forma, a análise torna-se importante para responder a questão: Como a cultura de vigilância digital pode impactar a privacidade dos usuários do Instagram? Um dos empecilhos encontrados para a realização desta análise se dá ao fato de ainda existirem poucas análises semelhantes em estudos acadêmicos que problematizam a utilização de dados pessoais e violação de privacidade em redes sociais, em especial sobre o Instagram.

Para chegar a este fim, optou-se pela realização de uma pesquisa exploratória com a utilização da análise documental da Política de Dados do Instagram como fonte primária, juntamente com as reflexões adquiridas a partir da revisão teórica desenvolvida ao longo do artigo. Para Gil (2008, p. 27), as pesquisas exploratórias abordam temas ainda pouco explorados para que possam ser estudados posteriormente. Diante disto, com os resultados obtidos será possível concluir como

[20] "*The Global State of Digital 2022*". Disponível em <https://www.hootsuite.com/pt/recursos/digital-trends>. Acesso em: 29 mar. 2022.
[21] Política de Dados do Instagram. Disponível em <https://www.facebook.com/help/instagram/519522125107875/?maybe_redirect_pol=0> Acesso em: 29 mar. 2022.

a cultura da vigilância digital pode impactar a privacidade ao utilizar os dados pessoais de seus usuários.

> A análise documental, muito mais que localizar, identificar, organizar e avaliar texto, som, imagem, funciona como expediente eficaz para contextualizar fatos, situações, momentos. Consegue dessa maneira introduzir novas perspectivas em outros ambientes, sem deixar de respeitar a substância original dos documentos (MOREIRA, 2005, p. 276).

Sendo assim, a primeira etapa da análise consistiu em uma leitura inicial do objeto de pesquisa para compreender quais partes seriam mais relevantes para o artigo. A Política de Dados é dividida em nove tópicos e foram escolhidos quatro deles: “Quais tipos de informações coletamos?”, “Como usamos estas informações?”, “Como estas informações são compartilhadas?” e “Como faço para gerenciar ou excluir informações sobre mim?”. Todos os quatro abordam assuntos relevantes para a pesquisa e análise de acordo com o questionamento proposto pelo artigo.

Para a segunda etapa da pesquisa, foram definidos três eixos a serem analisados: (a) Monitoramento digital, aborda a forma como o ciclo do monitoramento das informações opera neste contexto; (b) Coleta e Capitalização, como a rede social fatura utilizando dados extraídos; (c) Autodeterminação informativa, como o usuário pode ser afetado e como gerir suas informações. Dentro desses eixos, parâmetros como clareza das informações, características da privacidade, formato de tratamento de dados e aspectos da vigilância digital foram observados.

A análise e interpretação foi realizada na plataforma Notion para destaque e pontuações que se provarem relevantes. Para Moreira (2005, p. 276), a análise documental consiste em uma investigação que percorre um conjunto de operações intelectuais por parte do pesquisador para descrição e representação da fonte original, ainda que encontre novas reflexões no documento. Para melhor entendimento e explicação, cada eixo foi ilustrado em planilhas elaboradas na plataforma “Planilhas Google”. É válido ressaltar que a versão de 04 de janeiro de 2022 da política, data de sua última revisão, foi a utilizada para esta análise.

6 - ANÁLISE DA POLÍTICA DE DADOS DO INSTAGRAM

Para o entendimento inicial, é importante esclarecer quais são os Produtos Meta, frequentemente mencionados ao longo da política, são eles: Facebook (incluindo o aplicativo Facebook para celular e o navegador no aplicativo); Meta View;

Messenger; Instagram (incluindo aplicativos como o Boomerang); Dispositivos de marca do Portal; Produtos Oculus (quando usados com uma conta do Facebook); Lojas; Spark AR; Audience Network da Meta; Aplicativos do NPE Team; Ferramentas da Meta para Empresas; Quaisquer outros recursos, aplicativos, tecnologias, softwares ou serviços oferecidos pela Meta Platforms, Inc. ou pela Meta Platforms Ireland Limited.

De acordo com Gil (2008, p.156), a análise após a coleta de dados possibilita o fornecimento de respostas ao problema proposto para a investigação e tem como objetivo organizar e sumariar as informações obtidas. Junto a isto, é necessária a interpretação para a procura mais ampla dos sentidos, realizado mediante aos conhecimentos teóricos já adquiridos anteriormente. Posto isto, a análise e interpretação da Política de Dados do Instagram serão executadas juntas ao longo deste capítulo.

6.1 - Monitoramento digital

A Lei Geral de Proteção de Dados[22] é a principal referência para a regulamentação do tratamento de dados pessoais no Brasil e que dispõe de limites no que tange o monitoramento digital. Naturalmente, a política tende a estar adequada para operação no Brasil, mas a compreensão desta é importante para entender que a regulamentação não impede o monitoramento em si.

Na Política de Dados do Instagram estão dispostas quais informações a Meta extrai de seus usuários e como estas são tratadas pela empresa no tópico “Quais tipos de informações coletamos”.

> Nossos sistemas processam automaticamente o conteúdo e as comunicações que você e outras pessoas fornecem a fim de analisar o contexto e o conteúdo incluído nesses itens para as finalidades descritas abaixo (Instagram, 2022).

As informações coletadas pelo Instagram e suas finalidades são especificadas na política e estão relacionadas na Tabela 1. A coluna “O que é coletado?” são trechos extraídos diretamente da política e “Qual a finalidade?” são as reflexões baseadas nas informações retiradas deste documento.

[22] Lei Geral de Proteção de Dados Pessoais. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 29 mar. 2022.

Tabela 1 - Informações coletadas e suas finalidades de acordo com a Política de Dados do Instagram

	O que é coletado?	**Qual a finalidade?**
Informações e conteúdo que você fornece	Isso pode incluir informações presentes ou sobre o conteúdo que você fornece (como metadados), como a localização de uma foto ou a data em que um arquivo foi criado. Isso pode incluir também o que você vê por meio dos recursos que fornecemos, como nossa câmera.	Essas são as informações básicas utilizadas para criar ou compartilhar conteúdos, enviar mensagens ou comunicar-se com outras pessoas.
Dados com proteções especiais	É possível optar por fornecer informações nos campos de perfil ou nos Acontecimentos do Facebook sobre a sua opção religiosa, preferência política, saúde ou por quem você "tem interesse".	Dados sensíveis possuem proteção especial de acordo com a LGPD e precisam ser tratadas com mais atenção por parte das empresas. Então, especialmente neste caso, a política deveria deixar claro como essas informações são protegidas.
Redes e conexões	Coletamos informações sobre as pessoas, as contas, as hashtags, os grupos e as Páginas do Facebook com os quais você se conecta e sobre como você interage com eles nos nossos Produtos, como as pessoas com quem você mais se comunica ou os grupos dos quais você faz parte. Também coletamos informações de contato caso você as carregue, sincronize ou importe de um dispositivo.	Tais informações são usadas para ajudar o usuário a encontrar pessoas que talvez conheça ou tenha interesses semelhantes.
Seu uso	Coletamos informações sobre como você usa nossos Produtos, como o tipo de conteúdo que você visualiza ou com o qual se envolve; os recursos que você usa; as ações que você realiza; as pessoas ou contas com que você interage; e o tempo, frequência e duração das suas atividades [...] Nós também coletamos informações sobre como você usa recursos como nossa câmera.	Estes dados são usados para oferecer, personalizar de acordo com cada usuário e aprimorar os Produtos da Meta.
Informações sobre transações realizadas nos nossos Produtos	[...] nós coletamos informações sobre a compra ou transação. Isso inclui informações de pagamento, como o seu número do cartão de crédito ou débito e outras informações sobre o cartão; outras informações de conta e autenticação; detalhes de cobrança, entrega e contato.	A finalidade não está diretamente especificada na política, mas pode-se assumir que as informações são necessárias para que a transação seja realizada.

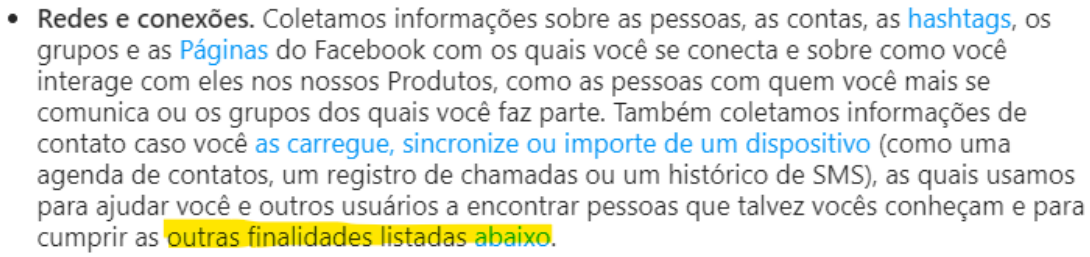
O que os outros fazem e informações que eles fornecem sobre você	Também recebemos e analisamos conteúdo, comunicações e informações que outras pessoas fornecem quando usam nossos Produtos. Isso pode incluir informações sobre você, como quando outras pessoas compartilham ou comentam uma foto sua, enviam uma mensagem a você ou carregam, sincronizam ou importam as suas informações de contato.	Não somente as informações que um único usuário produz são extraídas, mas também os dados que outros cedem acerca do dele.
Informações de dispositivo	Atributos do dispositivo, Operações do dispositivo, Identificadores, Sinais do dispositivo, Dados das configurações do dispositivo, Rede e conexões, Dados de Cookies	Desde o movimento do mouse até localização do GPS são coletados. A finalidade seria personalizar melhor os conteúdos, os recursos e para avaliar se o usuário realiza uma ação diferente ao visualizar um anúncio.

Fonte: elaborado pela autora.

Nas descrições de quais dados são coletados e suas finalidades já é perceptível a coleta massiva de dados do usuário, desde os mais básicos como nome, contatos e dispositivo, até os mais complexos como movimentação do mouse, dados sensíveis e informações de terceiros. Alguns tópicos são apenas subentendidos, deixando as especificidades da coleta ou da finalidade pouco claras. Como é o caso dos “dados com proteções especiais” que apenas indicam como o usuário pode optar por fornecer a informação ou não para outros perfis.

Um empecilho a ser avaliado se dá ao fato de que frequentemente a política apresenta links para informações mais específicas, mas não direciona para a informação a ser apresentada. Como no exemplo abaixo, em que o link não direciona para a “finalidade listada”, e sim para o início da política.

Figura 5 - Outras finalidades listadas abaixo



Fonte: Reprodução da Política de Dados do Instagram.

Paralelo a isto, todos os links específicos para as instruções acerca do Instagram estão em inglês, diferentemente dos links do Facebook que podem ser lidos em outras línguas, inclusive em português. Nesta mesma perspectiva, mesmo sendo a “Política de Dados do Instagram” o documento é voltado para a visão geral dos Produtos Meta e dificilmente para a rede social propriamente dita. Fator este que pode ser um empecilho para a execução do tratamento de dados de forma clara, já que cada um dos Produtos da Meta operam de formas diferentes uns dos outros.

Estes fatores apresentados, inclusive a respeito dos links apresentados na Figura 5, dificultam o entendimento e a acessibilidade do leitor às informações contidas no documento, aspecto essencial para tornar a política clara e de fácil acesso para todos os públicos.

Como mencionado anteriormente, Fernanda Bruno (2008, p. 12) define dois modelos de dados: os estáveis e os circunstanciais. O dado estável consiste nas informações com pouca ou nenhuma alteração no decorrer do tempo, como nome, dados geodemográficos, biométricos, entre outros. Já o dado circunstancial muda constantemente, são os dados comportamentais, transacionais, psicológicos, sociais, entre outros. Para a autora, essa segunda categoria é onde a vigilância digital é mais expressiva e pode-se notar nas coletas como “O que os outros fazem e informações que eles fornecem sobre você”, “Seu uso”, “Dados com proteções especiais” podem coletar dados que indicam emoções, tendências, comportamentos psicológicos e sociais do próprio usuário e também daqueles com quem ele se relaciona. É possível, até mesmo, validar a existência deste tipo de coleta como indicado na Figura 4 deste artigo.

A inovação, a personificação e a personalização são conceitos frequentemente usados para justificar a extração destes dados ao longo da política. Como citado anteriormente por Ana Frazão (2019), esta perspectiva utilitarista é usada para que tais justificativas se tornem aceitáveis para o uso da rede social e valem o comprometimento de direitos fundamentais, como o da privacidade. Ou seja, pode-se notar como os dados coletados são a “moeda de troca” entre o titular e a rede social, para que seja possível usufruir dos recursos do aplicativo.

Diante disto, a coleta massiva de dados implica no constante monitoramento das informações geradas no ambiente virtual, inclusive no Instagram. Como Zuboff

(2018, p. 18) bem explica, este big data é uma consequência inevitável de um rolo compressor tecnológico com vida própria, em que pessoas são apenas espectadores.

6.2 - Coleta e Capitalização

O faturamento principal do Instagram e outros Produtos da Meta tem sua origem na publicidade e anúncios distribuídos amplamente na plataforma, por mais que os dados pessoais não sejam vendidos em teoria. Uma pesquisa realizada em 2022 pela Opinion Box[23] com 1.600 usuários brasileiros do Instagram revela que 59% deles veem anúncios que têm a ver com ele. Isso se dá ao fato de que a Meta presta este apoio aos anunciantes e parceiros para medir a eficácia e a distribuição dos anúncios e serviços. Assim como, entender os tipos de pessoas que usam tais serviços e como elas interagem com os respectivos sites, aplicativos e serviços. Consequentemente, favorece este modelo de marketing direcionado a partir das coletas de dados.

Para uma melhor compreensão de como o Instagram retém este potencial de capitalizar os dados, uma tabela foi montada para apresentar quem são os agentes responsáveis por usar tais informações, assim como o que extraem da plataforma para seus interesses. Válido ressaltar que a coluna “O que coletam” são trechos retirados diretamente da política, mais especificamente do tópico “Como usamos estas informações”.

Tabela 2 - Compartilhamento com parceiros externos

Compartilhamento com parceiros externos	**O que coletam?**
Anunciantes	Fornecemos aos anunciantes relatórios sobre os tipos de pessoas que visualizaram os anúncios deles e sobre o desempenho de tais anúncios, mas não compartilhamos informações que identifiquem você pessoalmente (informações como seu nome ou endereço de email que possa ser usado por si só para contatar ou identificar você), a menos que você nos dê permissão para tanto.

[23] *Pesquisa sobre o Instagram no Brasil: dados de comportamento dos usuários, hábitos e preferências no uso do Instagram*. Disponível em <https://blog.opinionbox.com/pesquisa-instagram/>. Acesso em 08 abr. 2022.

Parceiros que usam nossos serviços de análise	Fornecemos estatísticas agregadas e insights que ajudam pessoas e empresas a entender como os usuários estão se engajando com as publicações, os classificados, as Páginas do Facebook, os vídeos e outros conteúdos delas dentro e fora dos Produtos da Meta. Por exemplo, administradores de Páginas do Facebook e perfis empresariais do Instagram recebem informações sobre o número de pessoas ou contas que viram as publicações deles, deixaram um comentário nelas ou reagiram a elas, bem como dados demográficos agregados e outras informações que os ajudam a entender as interações com a conta ou a Página do Facebook de cada um.
Parceiros de mensuração	Usamos as informações que temos (inclusive sua atividade fora de nossos Produtos, como os sites que você visita e os anúncios que você vê) para ajudar os anunciantes e outros parceiros a medir a eficácia e a distribuição dos anúncios e serviços deles, e também para entender os tipos de pessoas que usam tais serviços e como elas interagem com os respectivos sites, aplicativos e serviços.
Parceiros que oferecem bens e serviços nos nossos Produtos.	Quando você se inscreve para receber conteúdo premium, ou quando compra algo de um vendedor em nossos Produtos, o criador do conteúdo ou vendedor pode receber suas informações públicas e outras informações que você compartilhar com ele, bem como informações necessárias para concluir a transação, como detalhes de envio e contato.
Fornecedores e provedores de serviços	Fornecemos informações e conteúdo para fornecedores e provedores de serviços que viabilizam a operação de nosso negócio, seja fornecendo serviços de infraestrutura técnica, analisando como nossos Produtos são usados, oferecendo atendimento ao cliente, facilitando pagamentos ou realizando pesquisas.
Pesquisadores e acadêmicos	Também fornecemos informações e conteúdo a parceiros de pesquisa e acadêmicos para a realização de pesquisas que promovam conhecimento e inovação viabilizadores de nosso negócio ou missão e que intensifiquem a descoberta e a inovação acerca de tópicos de bem-estar social geral, avanço tecnológico, interesse público, saúde e bem-estar.

Fonte: elaborado pela autora.

Pode-se entender a partir da política que os anunciantes são aqueles que “contratam” a Meta para distribuir seus anúncios mais amplamente, já os parceiros se enquadram como pessoas ou empresas que utilizam das ferramentas disponibilizadas pela rede social para o fim que lhe interessar. De modo geral, a lógica da coleta de dados por parte dos anunciantes e parceiros gira em torno do marketing orientado. Ou seja, utilizar as informações adquiridas no ambiente digital para direcionar cada vez mais precisamente seus conteúdos. Logo, as curtidas, comentários, interações,

visualizações, dados demográficos e transações realizadas são coletados para esta finalidade.

No caso dos “parceiros de mensuração” nota-se que a coleta se estende até mesmo para fora dos produtos Meta. É importante ressaltar também que tais parceiros não são especificados, nem como operam, deixando a informação pouco clara ao leitor.

Quanto mais informações extraídas, melhor será a análise e utilização desses dados para um algoritmo mais preciso. Consequentemente este tratamento de dados permite maior vantagem competitiva no mercado para aqueles que usufruem das ferramentas disponibilizadas pelo Instagram e dos demais Produtos da Meta. Como reforçado por Zuboff (2018), nada é trivial ou efêmero na captura de *small data,* ou pequenas informações. “Esses dados são adquiridos, tornados abstratos, agregados, analisados, embalados, vendidos, analisados mais e mais e vendidos novamente” (ZUBOFF, 2018, p. 31).

Outra modalidade de compartilhamento de dados com parceiros externos é o caso dos “Pesquisadores e Acadêmicos”. Nesta ocasião, é válido relembrar do caso da Cambridge Analytica citado anteriormente, onde diversos dados extraídos para fins de pesquisa foram usados para a promoção da campanha de Donald Trump, um exemplo de como o tratamento de dados pode ser facilmente manipulado para fins antiéticos, além do lucro.

O risco a ser considerado é o mesmo mencionado por Ana Frazão (vide Figura 2) no Ciclo de Mercado de Dados em que a possibilidade do abuso do poder econômico através da extração de dados leve à violação da privacidade e manipulação do indivíduo, ocasionando em situações semelhantes ao da Cambridge Analytica. Carissa Véliz reforça esta ideia em entrevista para a BBC[24]:

> Neste momento, não somos tratados como iguais: não vemos o mesmo conteúdo online, não nos são oferecidas as mesmas oportunidades, muitas vezes não pagamos o mesmo preço pelos mesmos produtos — graças a algoritmos de sites da internet que usam nossos dados para nos oferecerem informações e produtos diferentes (VÉLIZ, 2021).

Esta perspectiva do tratamento de dados para fins de capitalização põe em risco o próprio titular das informações. Especialmente pelo fato de que o usuário do

[24] 'Falta de privacidade mata mais que terrorismo': o surpreendente alerta de professora de Oxford. Disponível em <https://www.bbc.com/portuguese/geral-54558878>. Acesso em 16 abr. 2022.

Instagram dificilmente tem ciência da realidade do algoritmo orientado e torna-se o objeto de lucro nesta relação.

6.3 - Autodeterminação informativa

Privacidade é ter domínio de como determinada informação pessoal circula. Como a autora Carissa Véliz (2021) reforça, privacidade é o poder que o usuário precisa ter para si mesmo e não o delegar para terceiros. É necessário buscar o domínio do circular das informações para que estas sejam acessíveis apenas às finalidades específicas.

> Logo, há uma transformação do conceito, que passa a abarcar não só o poder de exclusão, de impedimento de interferências alheias, mas também a centralidade do controle do indivíduo sobre suas informações pessoais, ou seja, sua autodeterminação informativa (COSTA E OLIVEIRA, 2019, p. 28-29).

Desta forma, a Tabela 3 traz todos os tópicos acerca do monitoramento digital da Tabela 1. Ou seja, a primeira coluna são os dados coletados apresentados na política e a coluna “autodeterminação informativa” avaliará se o usuário possui algum tipo de domínio com relação às próprias informações cedidas.

Tabela 3 - Autodeterminação informativa

	Autodeterminação informativa
Informações e conteúdo que você fornece	O usuário tem a possibilidade de configurar quem pode ver o que ele compartilha. Como, por exemplo, privar o perfil, bloquear outras pessoas, ocultar o status. Entretanto, esse controle não se estende à Meta. Ou seja, dados como localização, metadados, data, entre outros, continuam sendo coletados pela empresa.
Dados com proteções especiais	Da mesma forma, é possível ocultar os dados sensíveis do público externo, mas não da Meta.
Redes e conexões	Neste caso, o usuário pode optar por não sincronizar seus contatos com a rede social, limitando o acesso da Meta a algumas conexões. Entretanto, informações sobre as hashtags, contas e grupos continuam sendo monitoradas pela empresa.
Seu uso	Não é possível restringir este tipo de coleta de dados por parte do usuário.
Informações sobre transações realizadas nos nossos Produtos	Não é possível restringir este tipo de coleta de dados por parte do usuário. A limitação que poderia ser utilizada seria não realizar compras através da Meta.
O que os outros fazem e informações que eles fornecem sobre você	Neste caso, o usuário pode excluir um comentário indesejado ou retirar seu nome de alguma marcação de foto. Apenas não é possível restringir este tipo de coleta de dados em relação à

	Meta.
Informações de dispositivo	O aplicativo pede permissão para usar essas informações. Entretanto, caso o usuário não aceite, não é possível utilizar os recursos. Por exemplo, caso o acesso à câmera seja negado, o usuário não poderá utilizá-la.

Fonte: elaborado pela autora.

Diante do observado, pode-se perceber que o usuário possui diversos recursos para limitar sua visibilidade diante do público externo à Meta ou outros perfis. Ou seja, bloquear contas, ocultar suas informações, limitar comentários, privar o próprio perfil, entre outras opções. Entretanto, é quase impossível restringir o acesso da Meta às informações disponibilizadas pelo usuário. Praticamente todos os dados coletados permanecem sob domínio da empresa.

A Política de Dados também apresenta o tópico “Como faço para gerenciar ou excluir informações sobre mim?” que afirma conceder ao usuário a capacidade de acessar, retificar e apagar seus dados da rede social. Esta é uma das formas possíveis de limitar o acesso às informações do usuário por parte da Meta. A exclusão de determinados dados pode ser realizada, mas existe um período em que ficam reservados até a finalização de seu tratamento.

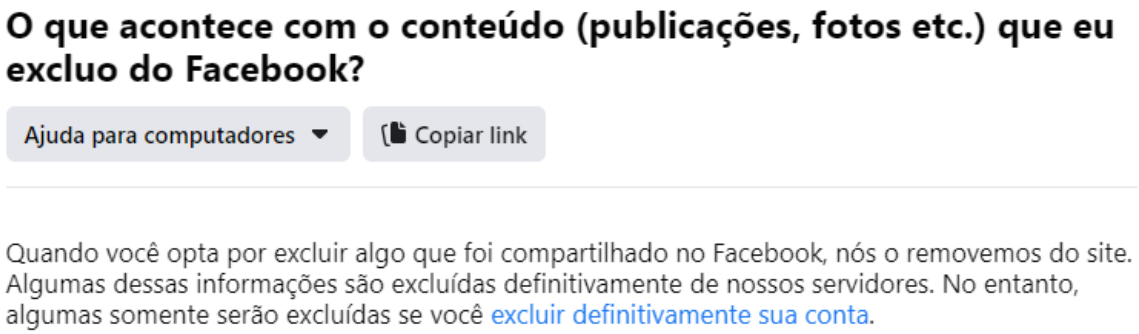
> Por exemplo, quando você pesquisa algo no Facebook, pode acessar e excluir essa consulta do seu histórico de pesquisa a qualquer momento, mas o registro dessa pesquisa será excluído após seis meses (INSTAGRAM, 2022).

Entretanto, cada caso pode variar de acordo com a natureza dos dados, do motivo pelo qual eles são coletados e tratados, e das necessidades de retenção operacional ou legal e estas variações não são especificadas na Política de Dados. Paralelo a isto, mesmo que o usuário venha a excluir determinados dados da rede social, seu uso sempre será limitado ou impossibilitado dependendo de qual informação ele opte por não ceder. Por exemplo, caso não permita a coleta de dados da câmera disponível no Instagram, não é possível utilizar o recurso.

Além disso, neste tópico sobre exclusão de informações, um dos links direciona para outra janela para explicar mais detalhadamente sobre o que acontece com os conteúdos excluídos da plataforma. É possível observar, conforme imagem abaixo, que determinadas informações coletadas só serão excluídas definitivamente se o

perfil inteiro for excluído também. Mais uma vez, a política não especifica qual situação caberia neste caso.

Figura 6 - O que acontece com o conteúdo excluído



Fonte: Política de Dados do Instagram.

De fato, existe uma inclinação própria do usuário a disponibilizar seus dados na internet, conforme estudado por Sibilia (2016). Entretanto, a ideia da privacidade deve ser ampliada para além da visão dicotômica entre a “casa-fortaleza” - aquilo que está guardado e seguro - e “casa-vitrine” - o que está exposto para todos observarem (RODOTÀ, 2008, p.25). Nesta linha de raciocínio, percebe-se que não necessariamente o que está na “fortaleza” está privado e seguro de abuso e o que está na “vitrine” também deve ter suas garantias de proteção, apesar de exposto.

Por mais que a coleta de determinadas informações possam ser justificadas para o uso da rede social, existe um problema a ser levantado que é a falta de clareza acerca de como são tratadas em alguns casos como observado no capítulo sobre o Monitoramento Digital e a falta de domínio que o usuário tem sobre suas próprias informações no que tange a coleta e tratamento de dados por parte da Meta.

7 - CONCLUSÃO

O cenário de vigilância e monitoramento está em constante mutação e evolução e a proteção da privacidade deve acompanhar este processo. Diante disto, este artigo se propôs a responder como a cultura de vigilância digital pode impactar a privacidade dos usuários do Instagram. Tendo como principal objetivo, entender quais são os dados coletados e como são tratados através da Política de Dados do Instagram. Para este fim, os aspectos do monitoramento no contexto da cultura de

vigilância digital, as características de capitalização de dados pessoais e como a privacidade se enquadra neste cenário foram estudados.

De acordo com a análise e interpretação realizadas através da Política de Dados do Instagram, concluiu-se que esta rede social, a 4ª mais usada no mundo, possui um sistema de coleta de dados consideravelmente extenso. Mesmo que esteja de acordo com a Lei Geral de Proteção de Dados, o monitoramento digital é expressivo e com diversas nuances e domínio acerca de dados pessoais de todos os tipos, desde os estáveis até os mais circunstanciais.

As finalidades das coletas de dados nem sempre são claras, por deixar seus objetivos apenas subentendidos para o leitor. Além disso, outro fator que pode prejudicar o entendimento e compreensão completa da política se dá na falta de acessibilidade em alguns momentos por disponibilizar informações importantes apenas em inglês.

Juntamente a isto, esta Política de Dados do Instagram não é específica para a rede social, mas abrange outros Produtos Meta também. Ou seja, nem sempre a operação do tratamento de dados pessoais são especificadas de acordo com as peculiaridades e características do Instagram, mas apenas relacionada de um modo geral.

Quanto à capitalização dos dados, pode-se entender na política que o dado propriamente dito não é vendido. Entretanto, o lucro se dá através do algoritmo orientado de anúncios e parceiros, em que todas as informações observadas no monitoramento digital podem ser usadas para fins mercadológicos.

Por fim, a privacidade neste contexto está em uma perigosa relação no contexto da vigilância digital. O titular dos dados tem pouco domínio de como suas informações circulam ou em como a Meta trata seus dados pessoais. Uma das poucas soluções de limitar o acesso da empresa seria a alternativa mais extrema de excluir o perfil completamente da rede social.

Os dados pessoais dizem respeito ao contexto existencial do próprio usuário e a proteção e privacidade deste devem estar fundamentadas no princípio básico de seus direitos. “Ele precisa estar ciente sobre como seus dados podem ser utilizados por entes públicos e privados e participar de forma mais ativa desse processo” (COSTA E OLIVEIRA, 2019, p. 38). Diante do estudado, é possível visualizar como a ampla proteção da privacidade diante da sociedade digital deve ir além da ideia

tradicional e buscar colocar o controle dos dados pessoais de volta ao domínio do titular.

REFERÊNCIAS

BBC. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. **BBC News**. Brasil, 20 mar. 2018. Disponível em <https://www.bbc.com/portuguese/internacional-43461751>. Acesso em: 09 mar. 2022.

BECK, Cesar; FORNASIER, Mateus. Cambridge Analytica: Escândalo, Legado e Possíveis Futuros para a Democracia**. Revista Direito em Debate**, Rio Grande do Sul, nº 53, p. 182-195, jan./jun., 2020. Disponível em <https://www.revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/10033>. Acesso em: 11 mar. 2022.

BLOOMBERG. Por dados, Meta ameaça tirar Facebook e Instagram da Europa. **Exame**, 07 fev. 2022. Disponível em <https://exame.com/negocios/por-dados-meta-ameaca-tirar-facebook-e-instagram-da-europa/>. Acesso em: 09 mar. 2022.

BRASIL, **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República [2018]. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 09 mar. 2022.

BRUNO, Fernanda. Monitoramento, classificação e controle nos dispositivos de vigilância digital. **Revista FAMECOS**, Porto Alegre, nº36, p. 10-16, ago. 2008. Disponível em <https://revistaseletronicas.pucrs.br/ojs/index.php/revistafamecos/article/view/4410/3309>. Acesso em: 29 mar. 2022.

CASTRO, Gustavo; OLIVIERI, Alejandro. A sociedade digital de extração de dados e os desafios para a democracia. **Revista Processus de Políticas Públicas e Desenvolvimento Social**, Brasília, vol. III, n.6, p. 16-40. jul-dez., 2021. Disponível em

<http://periodicos.processus.com.br/index.php/ppds/article/view/349/433>. Acesso em: 10 mar. 2022.

COSTA, Ramon; OLIVEIRA, Rodrigues. Os direitos de personalidade frente à sociedade de vigilância: privacidade, proteção de dados pessoais e consentimento nas redes sociais. **Revista Brasileira de Direito Civil em Perspectiva,** Belém, v.5, nº2, p. 22-41, jul./dez. 2019.

D'ANGELO, Pedro. Pesquisa sobre o Instagram no Brasil: dados de comportamento dos usuários, hábitos e preferências no uso do Instagram. **Opinion Box**. Minas Gerais, 14 fev. 2022. Disponível em <https://blog.opinionbox.com/pesquisa-instagram/> . Acesso em: 08 abr. 2022.

FEDERAL TRADE COMMISSION. **Data Brokers. A Call for transparency and accountability**. Estados Unidos. 2014. Disponível em: <www.ftc.gov/system/files/documents/reports/data- -brokers-call-transparency-accountability-report-federal-trade-commission-may- -2014/140527databrokerreport.pdf>. Acesso em: 10 mar. 2022.

FRAZÃO, Ana *et al*. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 1ª ed. São Paulo: Thomson Reuters Brasil Conteúdo e Tecnologia LTDA, 2019.

GARTNER. **Gartner Glossary**. Definição de Big Data. Gartner, c2022. Disponível em <https://www.gartner.com/en/information-technology/glossary/big-data> Acesso em: 09 mar. 2022.

GIL, Antônio. **Métodos e técnicas de pesquisa social.** 6ª ed. São Paulo: Atlas, 2008.

HOOTSUITE; WE ARE SOCIAL. **The Global State of Digital 2022.** Relatório global do uso da internet. HootSuite, c2022. Disponível em <https://www.hootsuite.com/pt/recursos/digital-trends>. Acesso em: 29 mar. 2022.

INSTAGRAM. **Política de Dados do Instagram.** Facebook. c2022. Disponível em <https://www.facebook.com/help/instagram/519522125107875/?maybe_redirect_pol=0> . Acesso em: 29 mar. 2022.

INSTAGRAM. **Termos de Uso**. Facebook. c2022. Disponível em <https://www.facebook.com/help/instagram/581066165581870/?helpref=hc_fnav&_rdc=1&_rdr>. Acesso em: 14 mar. 2022.

LATTO, Nica. **Data Brokers: Tudo o que você precisa saber.** *In:* Avast. **AVAST.** Brasil, 17 dez. 2021. Disponível em <https://www.avast.com/pt-br/c-data-brokers> Acesso em: 11 mar. 2022.

LISSARDY, Gerardo. 'Despreparada para a era digital, a democracia está sendo destruída', afirma guru do 'big data'. **BBC News**, New York, 9 abr. 2017. Disponível em <https://www.bbc.com/portuguese/geral-39535650> Acesso em: 10 mar. 2022.

LYON, David. Cultura da Vigilância: Envolvimento, exposição e ética na modernidade digital. *In:* BRUNO, Fernanda *et al* (Org.). **Tecnopolíticas da vigilância: Perspectivas da margem.** São Paulo: Boitempo, 2018. p. 151-179.

LYON, David. **The Electronic Eye: The Rise of Surveillance Society.** NED-New edition. University of Minnesota Press, 1994.

MOREIRA, Sonia. Análise Documental como método e como técnica. *In:* DUARTE, Jorge; BARROS, Antônio (Org.). **Métodos e técnicas de pesquisa em comunicação**. 1 ed. São Paulo: Atlas, 2005. p. 269-279.

ORACLE. **O que é Ciência de Dados?** Descrição sobre a Ciência de Dados. Oracle, c2022. Disponível em <https://www.oracle.com/br/data-science/what-is-data-science/>. Acesso em: 09 mar. 2022.

ORWELL, George. **1984**. 1ª ed. São Paulo: Companhia das Letras. 2009.

POZZI, Sandro. EUA multam Facebook em 5 bilhões de dólares por violar privacidade dos usuários. **El País**, New York, 13 jul. 2019. Disponível em <https://brasil.elpais.com/brasil/2019/07/12/economia/1562962870_283549.html>. Acesso em: 09 mar. 2022.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

SIBILIA, Paula. **O show do eu**. 2ª ed. Rio de Janeiro, Contraponto Editora, 2016.

SOLOVE, Daniel. J. **Digital person: technology and privacy in the information age**. New York: New York University Press, 2006.

THE ECONOMIST. **The World's most valuable resource.** Capa da revista. The Economist, c2022. 06 mai. 2017. Disponível em <https://www.economist.com/weeklyedition/2017-05-06> Acesso em: 10 mar. 2022.

VELASCO, Irene. 'Falta de privacidade mata mais que terrorismo': o surpreendente alerta de professora de Oxford. **BBC News**, Madrid, 16 out. 2020. Disponível em <https://www.bbc.com/portuguese/geral-54558878>. Acesso em: 16 abr. 2022.

VÉLIZ, Carissa. **Privacidade é Poder**. 1ª ed. São Paulo: Editora Contracorrente, 2021.

ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. *In:* BRUNO, Fernanda *et al* (Org.). **Tecnopolíticas da vigilância: Perspectivas da margem.** São Paulo: Boitempo, 2018. p. 17-68.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**. 1ª ed. New York: Public Affairs, 2019.